

**U.S. Department of Justice**



SLT:TJS

*United States Attorney  
Eastern District of New York*

*271 Cadman Plaza East  
Brooklyn, New York 11201*

June 21, 2013

BY Hand and ECF

Honorable Raymond J. Dearie  
Senior United States District Judge  
Eastern District of New York  
225 Cadman Plaza East  
Brooklyn, New York 11201

Re: United States v. Bebars Baslan,  
Criminal Docket 13-220 (RJD)\_\_\_\_\_

Dear Judge Dearie:

I respectfully write in response to the defendant's "status update", dated June 9, 2013, which contains several factual inaccuracies. As directed in the Court's Order, dated June 13, 2013, the government will confer with defense counsel. However, the government nonetheless submits this letter so that the record is clear regarding the discovery the government has provided to date and the government's inability due to technical and legal constraints to provide the copies of all electronic data "sanitized" of child pornography.

I. Factual Background

On or about February 13, 2013, a Confidential Source ("CS 1") reported to the FBI that an associate of CS 1, Bebars Baslan and Baslan's girlfriend, Kristen Henry, possess child pornography and were preparing to sexually exploit children. CS 1 indicated that Baslan told CS 1 that Baslan and Henry planned on opening a babysitting business as a cover to drug and sexually abuse children. Baslan also asked CS 1 to provide Baslan with access to children known to CS 1 so that Baslan and Henry could abuse them. Following February 13, 2013, CS 1 made numerous consensually recorded telephone calls with Baslan.

During these telephone calls Baslan discussed child pornography and the sexual abuse of children.

On March 7, 2013, CS 1 met Baslan at Baslan's residence. CS 1 was equipped by the FBI with electronic monitoring devices including audio and video recorders. During that meeting, Baslan used his computer to access child pornography which he played on his television while Henry and CS 1 were present. Some of the child pornography videos were captured on the video recording device provided to CS 1 by the FBI. The videos appeared to depict prepubescent girls being vaginally and orally penetrated by adult men's penises. Some of the videos had sound, and the children can be heard. Baslan described to CS 1 that the child pornography in his residence can be accessed on his iPad, iPhone, and television, and that the devices were accessing the child pornography from a central location. Baslan told CS 1 that he uses encryption that he created and that his files are "unhackable."

Over the course of the next week and a half, CS 1 had a number of additional consensually recorded telephone calls and meetings with Baslan. During the course of these communications, Baslan and CS 1 agree that, on March 19, 2013, they will meet at a hotel located in Jersey City, New Jersey where CS 1 will provide three children, with approximate ages of three months, eighteen months and eight years old so that Baslan and Henry can sexually abuse them. On March 19, 2013, Baslan and Henry traveled to the Jersey City hotel and knocked on the door that they believed to be occupied by CS 1. After CS 1 let them into the room, special agents of the Federal Bureau of Investigation ("FBI") arrested both Baslan and Henry. Baslan and Henry were arraigned the following day on a complaint charging travel across state lines to engage in sexual contact with a minor less than 12 years old, in violation of 18 U.S.C. § 2241(c).

During searches of Baslan and Henry incident to arrest, agents discovered a laptop computer, two Sony digital cameras, an 8 GB SD card, a 4 GB SD card, two iPhones, and a cellular modem. On April 1, 2013, the Honorable Robert M. Levy issued a search warrant for the devices seized during the course of Baslan and Henry's arrests.

Following the arrests of Baslan and Henry on March 19, 2013, agents also executed a search warrant, issued by the Honorable Roanne L. Mann, on Baslan and Henry's residence. During the course of the search, agents seized over 50 pieces of

electronic evidence. A log of the evidence seized from Baslan and Henry's residence is attached as Exhibit A.

In total, the evidence seized at the time of Baslan and Henry's arrest and from their residence includes five computers, three tablet computers, over a dozen internal and external hard drives, and numerous SD cards and removable flash memory storage devices. The combined electronic evidence consists of over 30 terabytes of digital storage.

The electronic evidence also contains encrypted information. Specifically, one hard drive seized from the residence was a one terabyte hardware encrypted drive equipped with a keypad. In normal operation, a code would have to be entered before the drive could be accessed. In May 2013, the FBI successfully circumvented the hardware encryption and discovered approximately 74,000 images of child pornography and 2,000 videos containing child pornography. The hard drive also contained an approximately 50 gigabyte file that was further encrypted and which the government has not yet been able to circumvent.

## II. Discovery Provided To Date

On May 9, 2013, the government produced initial discovery in this case. That discovery included copies of legal applications, documents seized from the defendants, documents obtained from other sources, and an inventory of the electronic evidence seized from the defendants' residence. Discovery also included a copy of 46 audio files of consensually recorded telephone calls, 8 audio files of consensually recorded meetings, and 9 videos of consensually recorded meetings. These amount to all consensually recorded audio and video in the possession of the government, with the exception of video of a meeting on March 7, 2013 between the confidential informant and defendants that contains child pornography. The government also produced data from the iPhones seized from Baslan and Henry at the time of arrest. The discovery letter accompanying those items is attached as Exhibit B. The government also produced statements made by Baslan and Henry to each defendant under separate cover.

Baslan objects that the government failed to produce numerous items of discovery. Specifically, Baslan indicates that the "PhoneMemo" application of his iPhone was omitted from discovery. The government uses forensic software to retrieve data from the iPhone, but that software does not capture all

data contained in every application on the iPhone. The government is currently attempting to copy the "PhoneMemo" application contents using another means. Though, the government notes that, based on a review of the physical iPhone, the last "PhoneMemo" recording is from December 2012, months before the activities noted in the complaint.

Baslan also objects that the government failed to provide the recordings on which the complaint is based. That is incorrect. The government has, in fact, provided those items. Finally, Baslan also objects that the government has failed to provide a copy of the approximately 30 terabytes of seized electronic evidence which has been sanitized of child pornography. As set forth below, it is not possible for the government to provide a sanitized copy of the electronic evidence in this case.

### III. The Government Is Legally and Technically Unable to Produce a Sanitized Copy of the Electronic Evidence

#### A. The Government Cannot Legally Provide Copies of Electronic Evidence Containing Child Pornography

Section 504 of the Adam Walsh Child Protection and Safety Act, codified at 18 U.S.C. § 3509(m), provides that material constituting child pornography "shall remain in the care, custody, and control of either the Government or the court." Section 3509(m)(2)(A) provides:

Notwithstanding Rule 16 of the Federal Rules of Criminal Procedure, a court shall deny, in any criminal proceeding, any request by the defendant to copy, photograph, duplicate, or otherwise reproduce any property or material that constitutes child pornography . . . so long as the Government makes the property or material reasonably available to the defendant.

(Emphasis added). Under § 3509(m)(2)(B), material is deemed to be reasonably available "if the Government provides ample opportunity for inspection, viewing, and examination" of the material at a government facility "by the defendant, his or her attorney, and any individual the defendant may seek to qualify to furnish expert testimony at trial." Courts in this District and others across the country have consistently and broadly upheld the constitutionality of this "safety valve" provision against challenges by defendants. See United States v. Spivack,

528 F. Supp. 2d 103, 106 (E.D.N.Y. 2007) (upholding refusal to mandate production of a mirror image of a hard drive containing child pornography); United States v. Battaglia, No. 5:07cr0055, 2007 WL 1831108, at \*4-6 (N.D. Ohio June 25, 2007) (general inconvenience and extra costs for defense counsel of viewing images at government facility did not deprive defendant of an "ample opportunity" to examine discovery materials); United States v. O'Rourke, 470 F. Supp. 2d 1049, 1058 (D. Ariz. 2007) (lack of internet access and malware at government facilities did not amount to "a denial of due process or of an ample opportunity to inspect the hard drive" but rather an easily remedied "communication" problem).

B. The Government Cannot Guarantee the Elimination of All Child Pornography Files from a "Sanitized" Digital Copy of the Hard Drive

There is no method for identifying child pornography save having a person physically review every file that could possibly contain child pornography. In this case, the government seized over thirty terabytes (over 31,457,280 megabytes) of data. This is amongst the most electronic storage seized in connection with any investigation by the Federal Bureau of Investigation New York Field Office for all types of crime. To illustrate the magnitude of the data seized, thirty terabytes of data could amount to over 7.5 million high-resolution images or the playtime of over a full year of non-stop DVD-quality movies.

To deliver a sanitized forensic copy of the hard drive to the defendant, each file in this highly voluminous data set would have to be individually viewed and analyzed to ensure that it is not contraband and that it is not being used to conceal contraband. Merely viewing the file would be insufficient to remove from consideration all of the possible ways that contraband could be stored. The forensic examiner would have to use several forensic tools and several different methodologies, none of which could be considered either trivial or complete.

It is important to note that contraband child pornography can be stored, encoded, or hidden in any file format. The search and analysis could not therefore rely on the accuracy of file extensions or file headers to locate the contraband because this information can be easily manipulated for concealment. It would be insufficient for a forensic examiner to search only through the hundreds of file formats like .jpg, .bmp, .gif, and .tif that are used specifically for

images. Rather, contraband images can be contained in almost any file formats. For example images may be saved in a container file, like a .zip file, attached to an email file, or embedded within another file such as a Microsoft Word document that contains both text and embedded images. Contraband could also be hidden in deleted files, unallocated space, system files and file slack. There is an endless array of technical possibilities for concealing contraband.

The instant case presents additional concerns due to the complexity and sophistication of the encryption ciphers used by the defendant to conceal the data. Mr. Baslan is a highly skilled professional computer programmer adept in dozens of technical coding languages. It took over two and a half months for the FBI to crack the encryption on the defendant's external hard drive to reach the first 76,000 images of child pornography. More contraband images almost certainly remain. Even utilizing the best technology and manual skills available, producing a forensic copy of the defendant's thirty terabytes of data with all contraband images identified and removed would be an impossibly burdensome process that would command an undue amount of time and resources from the United States.

C. The Government Will Make the Hard Drives Reasonably Available to the Defendant

Under the law, the government is not required to redirect untold resources to overcome obstacles created by the defendant himself in providing discovery. Rather, pursuant to the Adam Walsh Act, the government is required to make the evidence "reasonably available." The Government will make the hard drives and all of the evidence they contain reasonably available to the defendant at government facilities. The government has provided the defense with an itemized list of electronic evidence in its possession. If the defense indicates any item or items on the list and provides hard drives of equal size, the government will make a forensic copy of the evidence onto those hard drives. The government will then arrange for the defendant and his attorney to view the evidence at the government's proffer rooms during business hours. Following any review, the government will maintain possession of the hard drives and any computer used to review the hard drives. At the conclusion of the case or at whatever time requested by the defendant, the government will erase the hard drives provided by the defense and the computer used to view the evidence and return them to the defense.

To further facilitate review, if the defendant identifies files or discrete sets of files that the government is able to determine do not contain child pornography, the government will copy those files onto digital media provided by the defendant.<sup>1</sup> This arrangement addresses the defendant's complaints and also accomplishes the Congressional goal of "protect[ing] children from repeat exploitation in child pornography by preventing the unnecessary distribution of child pornography." See Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, §§ 501(1)(B)-501(2) (2006).

The government will also make itself available to discuss any of these issues with defense counsel, who to date has not contacted the government either prior to submitting his status report or after.

Respectfully submitted,

LORETTA E. LYNCH  
UNITED STATES ATTORNEY  
EASTERN DISTRICT OF NEW YORK

By: \_\_\_\_\_/s/\_\_\_\_\_  
Tyler J. Smith  
Assistant U.S. Attorney  
718-254-6186

CC: Clerk of the Court (By ECF)  
Anthony J. Carridi, Esq.

1 The defendant indicates in his letter that defense counsel indicated to the government that the electronic evidence includes "informational bullet points of [the CI's] wrongful acts history." Def. Ltr. at 2. He objects that these have not been turned over as discovery. During the conversation between the undersigned Assistant and defense counsel, defense counsel did claim that such an item existed. The undersigned Assistant requested information that would allow the government to locate that item among the plentitude of electronic evidence, specifically the computer or hard drive on which those "bullet points" would be found and, if possible, a file path to that item. Defense counsel has not yet provided any information that would allow the government to locate those purported files and the government has not yet, independently, identified any files matching the description provided by the defendant.